南投縣立水里國民中學

資通安全維護計畫

版次：V2.0

修訂人核章	阮〇〇
單位主管核章	王〇〇
資安長核章	陳〇〇

中華民國 109 年 6 月 15 日

資通安全維護計畫

文件制/修訂紀錄表

文件版本	修訂日期	修訂內容	修訂單位	修訂人	核定人 （資安長）
V1.0(初版)	108年6月10日	新擬訂文件	水里國中	阮○○	陳○○
V2.0	109年6月15日	修訂文件內容	水里國中	阮○○	陳○○

目　　錄

壹、依據及目的

本計畫依據下列法規訂定：

一、資通安全管理法第 10 條及其施行細則第 6 條。

二、南投縣政府資通安全維護計畫。

貳、適用範圍

本計畫適用範圍涵蓋南投縣立水里國民中學(以下簡稱本校)。

參、核心業務及重要性

一、 核心業務及重要性：

本校之核心業務及說明如下表：

核心業務	業務失效影響說明	最大可容忍中斷時間
校務系統：包含學籍管理、成績管理、人事資料管理、學生輔導管理等（向上集中）	可能使本校部分業務中斷	由上級管理單位訂之
全球資訊網（向上集中）	可能使本校部分業務中斷	由上級管理單位訂之
公文整合資訊系統（南投縣政府）	影響機關行政效率	由上級管理單位訂之

二、 非核心業務及說明：

本校之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
學生健康資訊系統（教育部）	可能使本校部分業務中斷	由上級管理單位訂之
公文電子交換服務系統（南投縣政府）	電子公文無法即時送達機關，影響機關行政效率	由上級管理單位訂之
教育部電子郵件系統	郵件無法即時送達機關，影響機關行政效率	由上級管理單位訂之

肆、資通安全政策及目標

一、 資通安全政策

為使本校業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality)、完整性（Integrity）及可用性（Availability)，特制訂本政策如下，以供全體同仁共同遵循：

（一）應建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。

（二）應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。

（三）應強固資通系統之韌性，確保機關業務持續營運。

（四）應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本機關同仁之資通安全意識，本機關同仁亦應確實參與訓練。

（五）針對辦理資通安全業務有功人員應進行獎勵。

（六）勿開啟來路不明或無法明確辨識寄件人之電子郵件。

（七）禁止多人共用單一資通系統帳號。

（八）落實資通安全通報機制。

二、 資通安全目標

（一）適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

（二）達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。

三、 資通安全政策及目標之核定程序

資通安全政策由本校資訊業務承辦人簽陳資通安全長核定。

四、 資通安全政策及目標之宣導

（一）本校之資通安全政策及目標應每年透過教育訓練、內部會

議、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。

（二）本校應每年向利害關係人(例如 IT 服務供應商、與機關連線作業有關單位)進行資安政策及目標宣導，並檢視執行成效，宣導之方式可透過教育訓練、會議、網站進行。

五、 資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於資通安全管理審查會議中檢討其適切性。

伍、資通安全推動組織

一、 資通安全長

依本法第 11 條之規定，本校由校長為資通安全長，負責督導機關資通安全相關事項，其任務包括：

（一） 資通安全管理政策及目標之核定、核轉及督導。

（二） 資通安全責任之分配及協調。

（三） 資通安全資源分配。

（四） 資通安全防護措施之監督。

（五） 資通安全事件之檢討及監督。

（六） 資通安全相關規章與行政命令之核定。

（七） 資通安全維護計畫之核定。

（八） 其他資通安全事項之核定。

二、 資通安全推動小組

（一）組織

為推動本校之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各業務承辦人成立資通安全推動小組，其任務包括：

1.跨業務資通安全事項權責分工之協調。

2.應採用之資通安全技術、方法及程序之協調研議。

3.整體資通安全措施之協調研議。

4.資通安全計畫之協調研議。

5.其他重要資通安全事項之協調研議。

（二）分工及職掌

本校之資通安全推動小組依資通安全長之指示負責下列事項，本校資通安全推動小組分組人員名單及職掌應列冊(附件 1)，並適時更新：

1.資通安全政策及目標之研議。

2.訂定機關資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。

3.傳達機關資通安全政策與目標。

4.資通安全相關規章與程序、制度之執行。

5.資料及資通系統之安全防護事項之執行。

6.資通安全事件之通報及應變機制之執行。

7.其他資通安全事項之規劃與推動。

8.每年至少召開 1 次會議，提報資通安全事項執行情形。

陸、專職人力及經費配置

一、 專職(責)人力及資源之配置

（一）本校依資通安全責任等級分級辦法之規定，屬資通安全責任等級 D 級，設置一名正式人員兼辦資通安全業務負責本校之法遵業務、教育訓練及資通安全事件通報及應變等業務之推動。本校現有資通安全專責人員名單及職掌應列冊，並適時更新。

（二）本校之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。本校之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

（三）本校之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。

（四）專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

二、 經費之配置

（一）資通安全推動小組於規劃配置相關經費及資源時，應考量本校之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

（二）各單位如有資通安全資源之需求，應配合機關預算規劃期程向資通安全推動小組提出，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置。

（三）資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

柒、資訊及資通系統之盤點

一、 資訊及資通系統盤點

（一）本校每年辦理資訊及資通系統資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為資訊資產、軟體資產、實體資產、服務資產、人員資產、個資資產等。

（二）資訊及資通系統資產項目如下：

1. 硬體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。

2. 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。

3. 資訊資產：以數位或紙本等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等。

4. 支援服務資產：

(1)支援服務之相關人員。

(2)相關基礎設施級其他機關內部之支援服務，如電力、消防等。

（三）本校每二年應依資訊及資通系統盤點結果，製作「資訊及資通系統資產清冊」，欄位應包含：資訊系統名稱、業務屬性、資

訊系統安全等級、共同性系統、承辦（管理）單位等。

（四）資訊及資通系統之硬體資產應以標籤標示於設備明顯處，並由總務人員載明財產編號、保管人、廠牌、型號等資訊。

（五）各業務管理之資訊或資通設備如有異動，應即時通知資通安全推動小組更新資產清冊。

二、 機關資通安全責任等級分級

本校自行辦理資通業務，核心資訊系統均由上級或監督機關兼辦或代管，未維運自行或委外開發之資通系統，為資通安全責任等級D級機關。

捌、資通安全風險評估

一、 資通安全風險評估

1. 本校應每年針對資訊及資通設備資產進行風險評估。
2. 執行風險評估時應依據南投縣政府資訊安全維護計畫第捌點執行相關作業。
3. 本校應每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估。

玖、資通安全防護及控制措施

本校依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項，採行相關之防護及控制措施如下:

一、 資訊及資通系統之管理

（一）資訊及資通系統之使用

1. 本校同仁使用資訊及資通系統須遵守系統管理機關相關規範。
2. 本校同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。
3. 本校同仁使用資訊及資通系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。
4. 非本校同仁使用本校之資訊及資通系統，應確實遵守本校之相

關資通安全要求，且未經授權不得任意複製資訊。

5.對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

二、 存取控制與加密機制管理

（一）網路安全控管

1.本校之網路區域劃分如下：

(1)外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。

(2)非軍事區(DMZ)：放置機關對外服務伺服器之區段。

(3)內部區域網路（Local Area Network, LAN）：機關內部單位人員及內部伺服器使用之網路區段。

2.外部網路、非軍事區及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。

3.應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。

4.對於通過防火牆之來源端主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。

5.本校內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

6.對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。

7.使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

8.無線網路防護

(1)機密資料原則不得透過無線網路及設備存取、處理或傳送。

(2)無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。

(3) 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。

(4) 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

(二) 資通系統權限管理

1. 本校之資通系統應設置通行碼管理，通行碼之要求需滿足：

(1) 通行碼長度 8 碼以上。

(2) 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

(3) 使用者每 90 天應更換一次通行碼。

2. 使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

3. 使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

(三) 特權帳號之存取管理

1. 資通設備之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

2. 資通設備之特權帳號不得共用。

3. 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。

4. 資通設備之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

5. 資通設備之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

(四) 加密管理

1. 本校之機密資訊於儲存或傳輸時應進行加密。

2. 本校之加密保護措施應遵守下列規定：

(1) 應落實使用者更新加密裝置並備份金鑰。

(2) 應避免留存解密資訊。

(3) 一旦加密資訊具遭破解跡象，應立即更改之。

三、 作業與通訊安全管理

(一) 防範惡意軟體之控制措施

1. 本校之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

(1) 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

(2) 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。

(3) 確實執行網頁惡意軟體掃描。

2. 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。

3. 使用者不得私自使用已知或有嫌疑惡意之網站。

4. 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

(二) 遠距工作之安全措施

1. 本校資通系統之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經內部程序核可同意後始可開通。

2. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。

3. 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。

(1) 提供適當通訊設備，並指定遠端存取之方式。

(2) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

(3) 進行遠距工作時之安全監視。

(4) 遠距工作終止時之存取權限撤銷，並應返還相關設備。

（三）電子郵件安全管理

1.本校人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用。

2.電子郵件系統管理人應定期進行電子郵件帳號清查。

3.電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新。

4.使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。

5.原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。

6.使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。

7.使用者應確保電子郵件傳送時之傳遞正確性。

8.使用者使用電子郵件時，應注意電子簽章之要求事項。

9.本校應定期舉辦(或配合上級機關舉辦)電子郵件社交工程演練，並檢討執行情形。

（四）確保實體與環境安全措施

1.辦公室區域之實體與環境安全措施

(1)應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

(2)文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

(3)機密性及敏感性資訊，不使用或下班時應該上鎖。

(4)機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。

(5)顯示存放機密資訊或具處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。

(6)資訊或資通系統相關設備，未經管理人授權，不得被帶離辦

公室。

（五）資料備份

1.重要資料應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。

2.本校應每年確認重要資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通設備。

3.敏感或機密性資訊之備份應加密保護。

（六）媒體防護措施

1.使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。

2.資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。

3.為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。

4.對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

（七）電腦使用之安全管理

1.電腦、業務系統或自然人憑證，若超過15分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。

2.禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

3.連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

4.筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

5.下班時應關閉電腦及螢幕電源。

6.如發現資安問題，應主動循機關之通報程序通報。

7.支援資訊作業的相關設施如影印機、傳真機等，應安置在適當

地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

（八）行動設備之安全管理

1.機密資料不得由未經許可之行動設備存取、處理或傳送。

2.機敏會議或場所不得攜帶未經許可之行動設備進入。

(九)即時通訊軟體之安全管理

1. 使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。

2. 因特殊需求須使用即時通訊軟體傳遞非機密之公務訊息時，應簽核至縣府一層長官同意後，方可開放，然大陸地區設計製造之即時通訊軟體仍不得使用。若中央訂有統一機關使用之即時通訊軟體，則應全面改用之。

四、 業務持續運作演練

依南投縣政府資通安全維護計畫第玖點第五項業務持續運作演練規定，本校為無核心資通系統，資通安全責任等級D級機關，無強制規定需持續運作演練，餘配合縣府規定辦理。

五、 資通安全防護設備

1.本校為提升資安防護，視資安狀況，應考慮建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級，其得由上級機關代為建置。

2.資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

壹拾、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本校應訂定資通安全事件通報、應變及演練相關機制。詳見本校所訂之資通安全事件通報及應變管理程序。

壹拾壹、資通安全情資之評估及因應

本校接獲資通安全情資，應評估該情資之內容，並視其對本校之影響、本校可接受之風險及本校之資源，決定最適當之因應方

式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、 資通安全情資之分類評估

本校接受資通安全情資後，應指定人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

（一）資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

（二）入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

（三）機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

（四）涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含機關內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

二、 資通安全情資之因應措施

本校於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

（一）資通安全相關之訊息情資

由資通安全推動小組彙整情資後進行風險評估，並依據資通安

全維護計畫之控制措施採行相應之風險預防機制。

（二）入侵攻擊情資

由指定人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

（三）機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

（四）涉及核心業務、核心資通系統之情資

資通安全推動小組應就涉及核心業務、核心資通系統之情資評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

壹拾貳、資通系統或服務委外辦理之管理

本校委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

一、 選任受託者應注意事項

（一）受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

（二）受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

（三）受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

（四）受託業務涉及國家機密者，應考量受託業務所涉及國家機密之機密等級內容，於招標公告、招標文件及契約中，註明受託者辦理該項業務人員及可能接觸該國家機密人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

（五）前點適任性查核得在必要範圍內就下列事項查核，查核前應

經當事人書面同意：

(1) 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案者。

(2) 曾任公務人員因違反相關安全保密規定，受懲戒處分、記過以上行政懲處者。

(3) 曾受到外國政府、大陸地區或香港、澳門官方之利誘、脅迫，從事不利國家安全或重大利益情事者。

(4) 其他與國家機密保護相關之具體項目。

二、 監督受託者資通安全維護情形應注意事項

（一）受託業務包括客製化資通系統開發者，受託者應提供該資通系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

（二）受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應 1 小時內通知委託機關及採行之補救措施。

1. 資訊資料遭洩漏。
2. 資訊系統遭竄改。
3. 系統之運作受影響或停頓。

（三）委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。

（四）受託者應採取之其他資通安全相關維護措施。

（五）本校應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

壹拾參、資通安全教育訓練

一、 資通安全教育訓練要求

（一）本校之一般使用者與主管，每人每年接受 3 小時以上之一般資通安全教育訓練。

二、 資通安全教育訓練辦理方式

（一）承辦單位應於每年年初，考量管理、業務及資訊等不同工作

類別之需求，擬定資通安全認知宣導及教育訓練計畫或配合縣府計畫，以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

（二）本校資通安全認知宣導及教育訓練之內容得包含：

1. 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。

2. 資通安全法令規定。

3. 資通安全作業內容。

4. 資通安全技術訓練。

（三）員工報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。

（四）資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

壹拾肆、公務機關所屬人員辦理業務涉及資通安全事項之考核機制

本校所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、南投縣政府暨所屬各機關學校公務人員平時獎懲標準表規定辦理之。

壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制

一、 資通安全維護計畫之實施

為落實本安全維護計畫，使本校之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本校之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

二、 資通安全維護計畫實施情形之稽核機制

本校應配合上級或監督機關之規定辦理查核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。

三、 資通安全維護計畫之持續精進及績效管理

（一）本校之資通安全推動小組配合縣政府計畫，於收到縣府公文

後 20 日內召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。

（二）管理審查議題應包含下列討論事項：

1.過往管理審查議案之處理狀態。

2.與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

3.資通安全維護計畫內容之適切性。

4.資通安全績效之回饋，包括：

（1）資通安全政策及目標之實施情形。

（2）資通安全人力及資源之配置之實施情形。

（3）資通安全防護及控制措施之實施情形。

（4）內外部稽核結果。

（5）不符合項目及矯正措施。

5.風險評鑑結果及風險處理計畫執行進度。

6.重大資通安全事件之處理及改善情形。

7.利害關係人之回饋。

8.持續改善之機會。

（三）持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

壹拾陸、資通安全維護計畫實施情形之提出

本校依據南投縣政府資通安全維護計畫第壹拾陸規定配合辦理，向監督機關-南投縣政府，提出資通安全維護計畫實施情形，使其得瞭解本校之年度資通安全計畫實施情形。

壹拾柒、相關法規、程序及表單

一、 相關法規及參考文件

（一）資通安全管理法

（二）資通安全管理法施行細則

（三）資通安全責任等級分級辦法

（四）資通安全事件通報及應變辦法

（五）資通安全情資分享辦法

（六）公務機關所屬人員資通安全事項獎懲辦法

（七）資訊系統風險評鑑參考指引

（八）政府資訊作業委外安全參考指引

（九）南投政府政府資訊安全管理要點

（十）南投縣政府資通安全緊急應變計畫暨作業處理程序

（十一）南投縣政府個人資料保護管理要點

（十二）南投縣政府資通安全處理小組設置及作業要點

（十三）南投縣政府資訊推動小組設置要點

（十四）南投縣資訊系統開發及維運作業要點

（十五）南投縣政府網路使用規範

（十六）南投縣政府電子郵件使用作業規定

（十七）南投縣政府網際網路網站管理要點

（十八）本校資通安全事件通報及應變管理程序

二、 附件表單

（一）資通安全推動小組成員及分工表

（二）資通安全保密同意書

（三）委外廠商執行人員保密切結書、保密同意書

（四）年度資通安全教育訓練計畫

（五）資通安全認知宣導及教育訓練簽到表

（六）資通安全維護計畫實施情形

（七）資通安全稽核計畫

（八）稽核項目紀錄表

（九）稽核結果紀錄表

（十）稽核結果及改善報告

附件表單(一) 資通安全推動小組成員及分工表

南投縣立水里國中

資通安全推動小組成員及分工表

編號：○○

製表日期：109 年 6 月 15 日

組別	單位職級	職掌事項	分機	代理人
策略規畫組	校長	資通安全長。執掌事項詳列於本校資通安全管理計畫中。	111	教務主任
	教務主任	1. 資通安全政策及目標之研議。 2. 訂定機關資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。 3. 依據資通安全目標擬定機關年度工作計畫。 4. 傳達機關資通安全政策與目標。 5. 辦理資通安全內部稽核。 6. 其他資通安全事項之規劃。	121	輔導主任
	輔導主任		151	教務主任
	網管教師		123	教務主任
資安防護管理組	學務主任	1. 資通安全技術研究、建置及評估相關事項。 2. 資通安全相關規章與程序、制度之執行。 3. 資訊及資通業務之盤點及風險評估。 4. 資料及資通業務之安全防護事項之執行。 5. 資通安全事件之通報及應變機制之執行。 6. 其他資通安全事項之辦理與推動。 7. 網管教師兼任策略規劃組顧問，並辦理資通行政業務。	131	總務主任
	總務主任		161	學務主任
	網管教師		123	教務主任
績效管理組	人事主任	1. 辦理資通安全內部稽核。	117	會計主任
	會計主任		118	人事主任

資通安全長：陳○○

附件表單(二)資通安全保密同意書-1

資通安全保密同意書（一般人員用）

本人_____自民國___年___月___日起，於_____服務，對於職務上所知悉或持有之機密資料、程式及檔案、媒體等，絕對保守機密，不任意對外洩漏，並能遵守個人資料保護法、國家機密保護法以及本府資訊安全管理要點等法令，如有違誤，願負法律上相關責任，離職後亦同。

具切結書人（簽章）：

戶籍地：

身分證字號：

中華民國　　年　　月　　日

附件表單(二)資通安全保密同意書-2

資通安全保密同意書（駐點人員用）

本人_____自民國___年___月___日起，於_____進行駐點服務，對於職務上所知悉或持有之機密資料、程式及檔案、媒體等，絕對保守機密，不任意對外洩漏，並能遵守個人資料保護法、國家機密保護法以及本府資訊安全管理要點等法令，如有違誤，願負法律上相關責任，離職後亦同。

具切結書人（簽章）：

戶籍地：

身分證字號：

中華民國　　年　　月　　日

附件表單(三)委外廠商執行人員保密切結書、保密同意書

資通安全保密切結書（委外廠商用）

具切結人_____，
於民國_____年參與「_____**案**」之規劃、設計或設備安裝，謹聲明恪遵契約之精神及規範如下：

一、對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經機關權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

二、本保密切結書不因立切結書人離職而失效。

三、立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

具切結人：

姓名及簽章	身分證字號	聯絡電話	戶籍地址
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

立切結書人所屬廠商：

廠商名稱及蓋章	廠商負責人姓名及簽章	廠商聯絡電話及地址
_____	_____	_____

說明：本切結書所蒐集之個人資料僅供本專案相關業務使用，並依個人資料保護法之相關規定，遵循本校資通安全管理規範妥為保存。

中　華　民　國　　年　　月

附件表單(四)年度資通安全教育訓練計畫

南投縣立水里國民中學○○○年度資通安全教育訓練計畫

壹、依據

南投縣立水里國中之資通安全維護計畫辦理。

貳、目的

為精進本校及所屬人員之資通安全意識及職能，並敦促該等人員得以瞭解並執行（本校）之資通安全維護計畫，以強化（本校）之資通安全管理能量，爰要求該等人員應接受資通安全之教育訓練，爰擬定本教育訓練計畫。

參、實施範圍（各機關自行定義）

本校所屬人員：

人員類別	人數
資通安全或資訊人員	○○
一般人員	○○
主管人員	○○
共計	○○

肆、訓練項目（各機關自行定義）

人員類別	訓練課程	時數
資通安全或資訊人員	電子郵件安全 ○○	○○
資通安全或資訊人員	資訊系統風險管理 ○○	
一般人員	資訊安全通識 ○○	○○
主管人員	○○	○○

伍、訓練期程

由各機關自行排定教育訓練期程。

陸、訓練方式

由各機關自行決定教育訓練方式(實體課程、線上課程…)。

附件表單(五)資通安全認知宣導及教育訓練簽到表

南投縣水里國中資通安全認知宣導及教育訓練簽到表

編號：○○○

課程名稱：資安宣導課程-案例分享、資安防護重點及社交工程等
時　　間：108 年○○月○○日 9：00 — 12：00
地　　點：＿＿會議室＿＿＿＿＿＿＿＿＿＿＿＿

單　位	職　稱	姓　名	簽　名
人事室	專員	○○○	
00 科	科員	○○○	

附件表單(六)資通安全維護計畫實施情形

南投縣水里國中資通安全維護計畫實施情形

編號：○○

本機關(單位)經主管機關核定後本單位之資通安全責任等級為 D級 ，依資通安全管理法第 12 條之規定，提出本(109)年度資通安全維護計畫實施情形、執行成果及相關說明如下表所示：

實施項目	實施內容	實施情形說明
1.核心業務及其重要性	1.1 核心業務及重要性盤點	本機關核心業務及重要性詳參資通安全維護計畫（詳附件，下同）。
2.資通安全政策及目標之訂定	2.1 資通安全政策訂定及核定	本機關已訂定資通安全政策，詳參資通安全維護計畫，並經資安長核定(詳公文附件)。
	2.2 資通安全目標之訂定	本機關已訂定資通安全目標，詳參資通安全維護計畫。
	2.3 資通安全政策及目標宣導	本機關為推動資通安全政策，已定期向同仁及利害關係人進行宣達。
	2.4 資通安全政策及目標定期檢視	本機關已定期召開資通安全管理審查會議中檢討資通安全政策及目標之適切性（詳會議記錄）。
3.設置資通安全推動組織	3.1 設定資通安全長	本機關已指定○○長為資通安全長，其職掌詳參資通安全維護計畫。
	3.2 設置資通安全推動小組	本機關已設置資通安全推動小組，其組織、分工及職常詳參資通安全維護計畫。
4.專責人力及經費之配置	4.1 專職(責)人員配置	本機關屬資安等級D級無須配置專職(責)人員。
	4.2 經費之配置	本機關今年視需求已合理分資安經費，資安經費佔資訊經費之○○%。
5.資訊及資通系統之盤點及核心資通系統、相關資產之標示	5.1 資訊及資通系統之盤點	本機關已於今年○月盤點本機關之資訊、資通系統，建立資產目錄。
	5.2 機關資通安全責任等級分級	本機關依資通安全責任等級分級辦法，為資通安全責任等級D級機關。
6.資通安全風險評估	6.1 資通安全風險評估	本機關已於今年○月完成本機關之資

		訊、資通系統及相關資產之風險分析評估及處理。
	6.2 資通安全風險之因應	本機關已依資通安全風險評估之結果擬定對應之資通安全防護及控制措施。
7. 資通安全防護及控制措施	7.1 資通安全防護及控制措施	本機關已依依安全維護計畫辦理，詳附件資料。
	7.1 資訊及通系統之保管	本機關已依依安全維護計畫辦理，詳附件資料。
	7.2 存取控制與加密機制管理	本機關已依依安全維護計畫辦理。
	7.3 作業及通訊安全管理	本機關已依依安全維護計畫辦理。
	7.4 系統獲取、開發及維護	本機關已依依安全維護計畫辦理。
	7.5 執行資通安全健診	本機關已依依安全維護計畫辦理。
8. 資通安全事件通報、應變及演練相關機制	8.1 訂定資通安全事件通報、應變及演練相關機制	本機關已依規定訂定資通安全事件通報應變程序。(詳附件)
	8.2 資通安全事件通報、應變及演練	本機關已依規定進行資通安全事件通報。 本機關已依規定於今年○、○月辦理社交工程演練，並於○月辦理通報應變演練。
9. 資通安全情資之評估及因應機制	9.1 資通安全情資之分類評估	本機關接受情資後，已進行分類評估。
	9.2 資通安全情資之因應措施	本機關已接受情資之分類，採取對應之因應措施。
10. 資通系統或服務委外辦理之管理	10.1 選任受託者應注意事項	本機關資通系統或服務委外辦理時，已將選任受託者應注意事項加入招標文件中。
	10.2 監督受託者資通安全維護情形應注意事項	本機關已依規定監督受託者資通安全維護情形，客製他資通系統開發者，已要求其出具安全性檢測證明….(請機關依實際情形列出)。
11. 資通安全教育訓練	11.1 資通安全教育訓練要求	本機關人員已規定進行資通安全教育訓練。
	11.2 辦理資通安全教育訓練	本機關已於今年○月辦理資通安全教育訓練。
12. 公務機關所屬人員辦理業務涉及資通安全事項之考核機制	12.1 訂定考核機制並進行考核	本機關已建立考核機制，並已依規定進行平時及年終考核。

13. 資通安全維護計畫及實施情形之持續精進及績效管理機制	13.1 資通安全維護計畫之實施	本機關已依規定訂定各階文件、流程、程序或控制措施，據以實施並保存相關之執行成果記錄。
	13.2 資通安全維護計畫實施情形之稽核機制	本機關已依規定辦理內部稽核。
	13.3 資通安全維護計畫之持續精進及績效管理	本機關已依規定辦理內部召開管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
其他說明		

承辦人：　　單位主管：　　資通安全長：

註：陳核層級請機關依需求調整

附件表單(七)資通安全稽核計畫

南投縣水里國中○○年度資通安全稽核計畫

壹、依據

一、南投縣水里國中之資通安全維護計畫辦理。

二、資通安全管理法第十三條規定辦理。

貳、目的

為瞭解本校資通安全維護計畫執行之有效性，爰擬定本稽核計畫，執行稽核作業。

參、稽核期程

自 108 年 0 月 0 日至 108 年 0 月 0 日。

肆、稽核範圍

全機關

伍、稽核項目及內容

依據各機關安全維護之內容，並參考國際資訊安全管理標準 ISO 27001:2013、國際資訊技術服務管理標準 ISO 20000、「個人資料保護法」、「個人資料保護法施行細則」、「政府機關(構)資通安全責任等級分級作業規定」或「資訊系統分級與資安防護基準作業規定」等，以及其他相關規定，由各機關自行定義當年度之稽核項目、內容及執行方式。

一、核心業務及其重要性

二、資通安全政策及目標

三、資通安全推動組織

四、專責人力及經費之配置

五、公務機關資通安全長之配置

六、資訊及資通系統之盤點，並標示核心資通系統及相關資產

七、資通安全風險評估

八、資通安全防護及控制措施

九、資通安全事件通報、應變及演練相關機制

十、資通安全情資之評估及因應機制

十一、資通系統或服務委外辦理之管理措施

十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制

十三、資通安全維護計畫及實施情形之持續精進及績效管理機制

陸、改善作業

由各機關自行評估對於稽核結果表現優良者是否給予行政獎勵，並針對缺失或待改善項目者研擬後續追蹤方式及頻率(如將前次稽核結果納入本次稽核範圍中追蹤辦理情形及進度)。

附件表單(八)稽核項目紀錄表

南投縣立水里國民中學稽核項目紀錄表

稽核日期：○○○年○○月○○日

稽核範圍：全機關

受稽核單位	稽核項目	稽核結果	備註
EX：總務科	資產盤點	■符合 □不符合 □不適用	經驗證其資產項目表，按規定進行資產盤點，各項資產均依規定建檔並指派責任人。
EX：人事室	權限控管	□符合 ■不符合 □不適用	可使用高權限登入A網站，提供一般同仁進行課程報到作業外，亦可查詢所有同仁之個人資料。
		■符合 □不符合 □不適用	
		■符合 □不符合 □不適用	
		■符合 □不符合 □不適用	
		■符合 □不符合 □不適用	
附註			
受稽核人員：○○○			受稽核單位主管：○○○

附件表單(九)稽核結果及改善報告

南投縣立水里國民中學稽核結果及改善報告

稽核範圍	全機關
稽核日期	107 年 ○○ 月 ○○ 日
審查日期	107 年 ○○ 月 ○○ 日

改善措施				
編號	**稽核缺失或待改善稽核項目**	**改善措施**	**改善期程規劃**	**相關證明資料**
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

承辦人:　　單位主管：　　資通安全長：

附件表單(十)改善績效追蹤報告

南投縣立水里國民中學改善績效追蹤報告

編號：○○

製表日期：○○○○

稽核發現			
稽核日期	108 年 10 月 20 日 08 時	受稽核單位	○○○
稽核區域	■ 電腦機房 委外業務之監督措施 自動備份系統之安全措施		
缺失或待改善項目與內容	待改善項目：電腦機房所設置之預備電源設備老舊。 缺失項目：委外廠商未定期為保養相關設備。		
影響範圍評估	將影響電腦機房之運作及相關非核心系統之線上服務之提供。		
發生原因分析	未落實監督委外廠商管理之責任。		

改善措施成效追蹤			
改善措施		預計成效	執行情況
管理面	定期進行委外廠商承辦人員之教育訓練，已落實對委外廠商之監督責任。	要求委外廠商每季進行保養，並提供相關保養紀錄。	已與委外廠商接洽。
技術面			

<table>
<tr><td>人力面</td><td></td><td colspan="2"></td><td></td></tr>
<tr><td>資源面</td><td>更新相關電腦機房設備，並確保備份設備及機制運作效果。</td><td colspan="2">電腦機房電源設備更新，並採用不斷電系統，於停電時可維持 12 小時運作。</td><td>已進行採購作業。</td></tr>
<tr><td>作業程序</td><td></td><td colspan="2"></td><td></td></tr>
<tr><td>其他</td><td></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="5">績效管考</td></tr>
<tr><td colspan="2">改善措施確認</td><td colspan="3">■合格／完成
□待追蹤(追蹤期限：＿＿＿＿年＿＿＿月＿＿＿日）
□不合格(說明：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿)</td></tr>
<tr><td colspan="2">經費需求或編列執行金額</td><td>○○○萬元。</td><td>經費執行情形</td><td>已進行相關電腦機房設備更新採購，共執行○○萬元。</td></tr>
<tr><td colspan="2">預定完成日期</td><td>106 年 11 月 20 日</td><td>實際完成日期</td><td>106 年 11 月 20 日</td></tr>
<tr><td colspan="2">完成進度或情形說明</td><td colspan="3">定期檢視委外廠商之監督維護責任。</td></tr>
<tr><td colspan="2">改善成效考核</td><td colspan="3"></td></tr>
<tr><td colspan="2">後續成效追蹤</td><td colspan="3"></td></tr>
<tr><td colspan="2">資通安全推動小組</td><td>○○○</td><td>資通安全長</td><td>○○○</td></tr>
</table>